

Being anonymous

- Written by anonymous

More people started using tor when they got to know that the government and companies are watching every activity they do online. They became aware about the privacy issues which came by using the products of big-tech companies, Facebook, Google, Microsoft, Amazon, and so on...

The least thing the people can do to protect their privacy is to stay away from the products and services of big corporations.

There are many activists out there who support ethical technology than that which disrespects it's users, like Richard Stallman (founder of GNU/Linux), Todd Weaver (founder and CEO of purism "social-purpose corporation").

When you want to protect your data, two things come first, whether you want privacy (or) anonymity. Privacy and anonymity are often merged together as "being not known to anyone". But it's wrong. If two persons, whose names are known, have sent messages to each other, and the messages are encrypted, that's privacy. If two messages (which are not encrypted) are sent by two mysterious people (whom we can't trace out), that's called anonymity.

Anonymity is common in hacker culture. Hackers and 'Tech-ists' truly know what it means to be anonymous.

Anonymity doesn't just mean hiding your real name when you are online.

Hiding your real name and using a pseudonym is a very small thing when it comes to anonymity. You need to do many other things as well for being anonymous (like being in disguise!).

Before we get deeper into the knowledge about privacy and anonymity, lets talk about some tools which respect the privacy and freedom of it's users.

1. First one is obviously, Tor. Tor hides your IP address from the websites that you visit and your internet service provider. If you are browsing the internet from normal browser like Firefox or chrome, your online activities can be seen by government and the ISP, they also send the information about you like your IP address, operating system that you are using, the browser you are using etc., With tor, the websites, Government, and ISP will have zero knowledge about

what you do online. Tor browser is available for Windows, Mac, Linux, Android, and IOS. When using Tor, make sure that you won't give away information about you like your real name, because in that way the websites will recognize that's it's you and you are using tor network.

2. Second is VPN (virtual private network). It is mostly used to access the websites that have been blocked in your region. But it is also a useful tool for protecting your privacy or anonymity. Like tor, VPN also hides your IP address from the sites you visit. But however, most VPN providers in the internet are not safe. They can keep logs of your browsing history in their servers. So make sure that you are using a trusted VPN service. It is recommend to use only tor browser with VPN because if you are using tor with VPN, the VPN provider will not know your browsing history. **Do not trust free VPNs when it comes to privacy. They might help you to access the sites that have been blocked in your country, but they keep permanent logs of you browsing history and use it to sell to advertisers.** So use a paid, and trusted VPN service.

3. Use completely free GNU/Linux operating systems. Here, free doesn't mean in terms of price; free means freedom. There are many GNU/Linus distributions out there which includes non-free packages in them. Don't use them! And don't use Windows or Mac even. These non-free proprietary operating systems are a threat to your privacy. I recommend using Pure OS because it is completely free, and it's emphasis is on privacy and security. However, if you want complete anonymity, use an operating system likes Qubes, Tails (portable), Whonix; these operating systems are pre-equipped with TOR to make sure that you are 100% anonymous.

Even famous Linux operating systems like Ubuntu and Manjaro include non-free proprietary packages in them.

If you are a beginner to Linux operating systems, use pure OS; it is easy to install and very beginner friendly.

Beware of articles in the internet about Linux distributions. They mostly talk about Ubuntu, a non-free operating system that disrespects the privacy and freedom of it's users.

You can find .iso file of Pure OS at pureos.net

4. Jami, Jitsi, Wire. These three are completely free messengers. However the most anonymous and private way to chat with others is to use tor chat or Ricochet. Messages sent using Tor chat and Ricochet are routed through tor network; and the most beautiful thing about them is that you don't need an account! You have to just exchange your unique user id with the person you want to chat with.

5. Recommended add-ons or extensions for browsers:

- a. https everywhere
- b. NoScript
- c. LibreJS
- d. Any reputed ad-blocker

note: Https everywhere and NoScript are bundled with Tor browser.

6. Search using DuckDuckGo or Startpage. These two search engines don't save your search history in their servers.

7. Used laptops and PCs. Second hand Laptops are highly recommended for those who want a high degree of anonymity. Just buy them, install a privacy respecting OS in it, that's it!

8. Use cash whenever and where ever possible. Your online transaction are always monitored by the government agencies so the most anonymous way to make a transaction is to use cash, or bitcoin.

9. The thought the being anonymous is the most powerful tool for being anonymous. Avoid the temptation to get into a normal life. Most of your friends and colleagues might force you to use a software that isn't free and privacy respecting. Don't do that! Instead say them about a free and privacy respecting alternative to it. So the most powerful tool for being anonymous is the thought of being anonymous.

10. Don't reveal too much about yourself, that's the concept of anonymity. Don't reveal your IP address, real name, phone number, email id, or any other minor things about YOU.

11. Privacy policy. Read the privacy policy before you sign-up for a service. If the privacy policy states that it collects the information about the users, and also use it for advertising, DON'T USE IT!

12. Do as less web-browsing as possible. Because the most perfect way to be anonymous online is to stay offline. Your grand ma is probably more anonymous than you are because she was not exposed to the internet ever in her life. "The world is beautiful offline".

13. Turn off everything in your mobile phone; Bluetooth, WI-Fi, and everything else. If possible, to stay 101% anonymous, don't use mobile phone. Because mobile can be used to track you using the cell-phone signal.

Now, the above mentioned tools and tips are just the beginning to your journey into anonymity. There are a lot more things to do for achieving anonymity. Even if one thing in all of the above fails, then you might be vulnerable to losing your anonymity.

Privacy comes with freedom

If a software doesn't give you freedom, it doesn't give privacy or anonymity. Many large tech companies impose restrictions on their products such that the users will not have freedom to use it the way they want to. For example, Facebook forces its users to give their real name, which is a threat to their personal privacy, and it uses your name to create an advertising profile and show you ads based on your interests.

Another example, Amazon only sells e-books in the Kindle format which means that users will not have freedom to convert to pdf, epub, html, or any other format. So don't buy books at Amazon. Go to a book store and buy it using cash only.

I'll now introduce to a new term called DRM (Digital Restrictions Management). DRM is a bad thing that exists in most of the audio and video streaming platforms. DRM restricts the users from downloading a file (downloading a file is different from viewing offline), sharing it, and modifying it. YouTube imposes DRM on its videos; such that the users cannot download a video, but can only view it offline; same happens with Netflix, Prime Video, and Spotify.

My recommendation is to not use any service (free or paid) that imposes DRM on its content. Also, the CEO of Disney once said *"if the consumers even know that DRM exists, then we wouldn't be in this position"*

To get access to DRM-free content in the internet, go to archive.org where you will find millions of audio, video, text files, and soft wares, everything for free! You can download them, share them, do it whatever you want to do it with them, and you will not be called as 'pirate'. For a DRM-free alternative to Spotify, use libre.fm; For a DRM-free alternative to Netflix and Prime Video, use free torrents (even pirated ones is okay!). Make sure that whatever you do, you do it on TOR.

The reason why I said privacy comes with Freedom is because if a software doesn't give freedom to do anything a user wants to do with the software, then the software is what controls the user; user doesn't control the software. It

might be using the user's data to collect data and do advertising with it. They treat users as a money mine.

YouTube can't earn money if every user downloads the videos and share it with others, same with other proprietary softwares also. The software that gives the users freedom to modify the software and use it the way they want to is called and Libre Software (Libre means freedom). So for being anonymous, use only Libre softwares, 100% Libre.

How proprietary, Non-Libre software is harmful to the people?

Well, there are many reasons for Proprietary softwares being harmful to people. A company whose motive is earning profits and maximizing the value of the shareholders will always choose profits over people.

For example, Facebook once targetted children (mostly teens) who were depressed and were kind of having suicidal thoughts and showed them the advertisements of the video games because the children who are prone to loneliness and depression are most likely to get addicted to the video games. In this injustice way, Facebook earned money from the video-game advertisers. Facebook created an illusion among the people to get a feeling of being connected using friendly and useful technology, when it's actually very dangerous. Many people are unaware about how much data Facebook collects from them. It can trace out key words from your conversations over phone calls and show you advertisements based on that! Facebook's face recognition implementation is dangerous to the people who are on Facebook, and off Facebook. It can use those faces to link the relationships between the people and enhance their advertisements targetting. So don't post picture of your friend or colleague on Facebook, or any of it's family or companies (Instagram, and Whatsapp). If you post, then you are probably doing something bad to them! Same happens with the face recognition software in Google. If you truly want to anonymous, don't let any of your photo back-up in Google Photos, Drive, or Dropbox even. These things can destroy your privacy and anonymity!

Proprietary softwares are often designed to be addictive. These big companies employ people called attention engineers which are specialised in making the online services addictive. These companies and advertisers fight for your attention and time. Any app whose user interface feels good might have employed attention engineer to make it look and feel good.

These online companies can manipulate your purchasing behaviour. You are followed by ads wherever you go in the internet. These ads, sometimes, have power to manipulate the way you think and live. They make your life sad and

unfulfilling because you are having material wants in your heart. For example, a car company will not advertise about the car, it will show a luxurious life that includes that car; which makes a consumer feel that to live a luxurious life, they need to buy that car.

The conclusion is that leaving the big E-Corps (evil corporations) behind will be good to your mental well-being, privacy and anonymity, and you will also be contributing for a good and ethical world.

Dark net- the beginning of your journey towards anonymity.

Dark net is the most beautiful place in the internet, also the most dangerous one. It contains the sale of drugs, weapons, child pornography and many other illegal things. But the dark net is not limited to only those things; it contains social networks, forums, messaging, file sharing etc. Every dark net site ends with .onion domain. When you first get into the dark net, you will observe that the websites are a series of long, random series of numbers and letters which are really hard to remember; for example, jiuhg7458jnksnaru9209fnj029yr.onion Remember, dark net can be accessed only with tor browser. For additional security, you can use VPN along with tor (A reputed VPN that doesn't keep logs).

Dark net is the place which everyone deserves to be. It respects your freedom, privacy, anonymity, and it doesn't follow you around with advertisements, pop-ups, and government and E-corps can't track you when you are using dark net. I highly recommend disabling JavaScript in TOR browser for high level of privacy and security.

If your goal is being anonymous, use TOR, only TOR.

[fact- Facebook also owns a .onion domain!, but I still don't trust it]

There are mail providers in dark net like Torbox and mail2tor. But the limitations of these e-mail providers are that you can send a mail only to someone who is using a Tor provided email service.

However I don't recommend using your personal email for creating not-so-important accounts. Instead, use guerrilla mail which provides temporary, disposable email for free. I recommend accessing guerrilla mail from TOR only, otherwise it might track your IP address.

Tools which use TOR to perform their actions.

Onion share: Onion share is file-sharing platform. The files are shared with the other person anonymously through TOR network.

Proton mail: The most popular anonymous e-mail provider made my scientists who met at CERN. It has e-mail encryption option. It has both dark net and

normal domain. For creating a proton mail account, It redirects you to it's normal site, which I recommend doing it only in tor. After that, you can log-in anytime in it's .onion domain: protonirockerxow.onion

Tor chat: all the message sent using Tor chat are routed through TOR network.

Galaxy 3: a popular social network on dark net [link: <http://galaxy3bhpzxecbywoa2j4tg43muepnhfalars4cce3fcx46qlc6t3id.onion/>]

Qubes, Tails, and Whonix: These three are the operating systems that are pre-equipped with tor. So when you use these operating systems, what happens on tor, stays on tor. There no way somebody could track you.

The web we know is not even 1% of the whole. World wide web is very small! The actual, uncensored, surveillance free internet is dark net. The world wide web consists of the websites that appears on the search results and a normal search engine like Google, DuckDuckGO. Deep web is what doesn't appear in the search results but exists. Dark net is what can be accessed only with tor. The following image explains it more clearly:



The internet we use everyday is called as surface web, it is very small. Deep web and Dark web take up the large portion of the internet. 90% of the darknet is advertisement free, 100% of the dark web is surveillance free and tracking free.

If you want to be anonymous, go and explore the dark web using tor with JavaScript disabled. You will get to know many things that you don't know exists. While using Dark web, don't give any small information about you, including your real name.

WARNING: If you've created an account on tor, then make sure that you don't log-in with normal browser as it might reveal that it's you. And if you've already created an account on normal browser, then there is no point of using it on tor browser. So always make sure that what you did on tor, stays on tor.

The only way internet can become a better place is by removing the surveillance, tracking, and advertisements. For this, more people should be

creating dark net sites instead of normal sites. Convince your friends to go dark. The power should not be in the hands of evil corps.

Dark net is safer place than the normal internet for many reasons that I have mentioned above. By going dark, you are doing something good to the society by not contributing your data to evil corps, and that's what I think everyone should do.

Ross Ulbricht- *a true hero!*

In the year 2011, there was a buzz word in the dark net called “silk road”. Silk road is a dark net e-commerce website which is used by sellers to sell various kind of drugs. It did not only sell drugs, it sold other legal items too, but mostly, they sold only drugs. It became the most popular online drug market in 2011. The government agencies were trying to find the owner of silk-road. But they couldn't do it till 2013. The owner of the silk road site used a pseudonym called “Dread Pirate Roberts”. It was clear that he did not intentionally create silk road for drugs marketing. He wanted to create a market place where anyone could sell and buy anything they want to unless it hurts anybody. Pirate Roberts created a page in silk road site convincing that drugs are harmful. He just created a market place, but it is buyers and sellers who converted it into a drugs market. He tried to be as anonymous as possible, until he was arrested by FBI in 2013. The actual name of Dread Pirate Roberts was Ross Ulbricht, a science and engineering graduate.

Ross was sitting in a Coffee shop and two FBI agents who pretended to be lover fought with each other to distract Ross, then the third FBI agent came from back and pulled Ross' laptop. They did this so that he won't delete the data. It is still not clear how the FBI agents found him thought Ross' used the most private and anonymous way to conduct a business.

Media depicted Ross as a money-minded, intentioned to harm others, person. But he is not. He is just like any other person with good intentions. He wanted to give freedom for both sellers and buyers to sell and buy anything they want to, without the interference of any third person, especially government.



He was sentenced to double life imprisonment and forty years without the possibility of parole.

Many of his friends and family members said that Ross' was the most calm, lovable, respecting person they have ever met. He has a philosophical mindset. He was very much interested in physics and the nature of the

universe. He was the first person to create a market place in the dark net. His friend loved him for his peaceful nature. If you want Ross' to be freed from imprisonment, you can sign the petition at freeross.org

The darknet has many other stories and heroes with many philosophies, primarily focused on freedom and privacy and anonymity of the people.

Jokes by evil corporations

1. "We protect your privacy" – Facebook, Google, Apple, Microsoft and many more... (well you don't protect our privacy)
2. "You can trust us" – all big corporations... (Well, you don't give us freedom to verify your source code)
3. "We are connecting you to your family, friends and interests"-- all big corporations...(We were peaceful only before you came into our lives. After you came, our minds have become frustrated.)
4. "We are creating an ethical technology to improve the lives of the people"-- all big corporations...(You are not improving our lives, you are destroying it! You are not creating ethical technology! Do you even know what the word ethical means?)

What's happening behind the screens?

Facebook made a secret deal with Amazon to give Amazon access to Facebook's data about users. The plague of both of those companies!

Amazon and Google are trying to bring their assistants to every possible household to gather more data about them.

Amazon keeps Alexa's recordings and keeps a transcript of it.

Warehouse workers at Amazon are forced to speed up and ignore the safety rules.

Apple censors that mails that people send.

Safari browser send the data to Chinese company Tencent.

Apple phones are designed to work only with batteries manufactured by Apple. Other batteries suck in Iphone.

Facebook banned the accounts that did not use real names.

Facebook encourages the users to give as much information as possible about them.

Facebook buys personal data from various data brokers.

Facebook scans the photo that is took in a phone through various technical methods.

Facebook snoops on the people's SMSes

Facebook is planning to track the movement of the mouse using malicious JavaScript.

Facebook can tell whether a user is asleep or not.

Facebook increased it's visible use of face recognition.

Facebook knowingly worked with game developers to encourage children to spend their parent's money.

Facebook will make people more lonely and depressed.

Many of the Google services require trivial JavaScript running in the browser.

Google stores a list of all the items a user has purchased to manipulate the consumer behaviour.

Many paid movie streaming website and software impose DRM on it's content.

These are only known bad things that these evils corporations do; There must be many other things that they did without the user's knowledge.

Disposable technology by evil corps.

Most of the electronic devices are designed to work for only few years; that's the reason they don't come with removable batteries nowadays. Most of the popular operating systems are having high resource requirements thus making the devices slow after some time.

When you install GNU/Linux (obviously a free one) in your old windows computer, you are giving a new life to it. Linux based operating systems have low resource requirements so they extend the life of a device.

Apple shows-off that it is serious about the environmental problems, so it has introduced recycle program. But only 1% of all the iPhone users are making use of the recycle program so there's no point of recycling.

These evils corps are causing a huge damage to the environment. They don't care about user privacy, freedom, anonymity, and environment, and protection of flora and fauna, all they care about is maximising the shareholders' value.

So I recommend everyone to ditch windows, mac, ios, android, and other non-free operating systems, to a completely free GNU/Linux operating systems.

If you are having an old windows computer which works very slow, install Tori OS in it and it will work like a new one!

The conclusion of this section is to not use any disposable technology designed by evil corps.

The pressure from the society-

A lot of pressure exists in the society to use non-free and privacy disrespecting software. For example, you may be forced to use WhatsApp for talking to your friends, and Zoom for conducting online meeting. To remove that pressure from society, we have to educate other people about using a free and privacy-respecting software. That's one of the reason I have written this book actually, to educate others about the use of free and privacy respecting software.

Mastering the art of Disguise, and other offline things to achieve anonymity.

This is the last part of being anonymous. For truly being anonymous you have a lot to do offline, being in Disguise is one of them. Disguise refers to changing your appearance such that nobody recognises you. This is a crucial step for being anonymous and saving yourself from



CCTV cameras that have face-recognition in them. For saving yourself from cameras, you may need to wear a mask, sunglasses, a cap. You can even grow a beard if you never had a beard before; shave off your head if you have never shaved; change the shape of your eyebrows; and a lots more cool things that can completely change the way you look. Always make sure that nobody posts a picture of you in the internet, when you are in disguise.

When you are introducing yourself to others, use a fake name. Only do things that lets you do anonymously; for example, a shopping mall might ask for your phone number, and other details, don't give them any information about you. And once again I'm reminding you, use only cash if you truly want to be anonymous. Don't use your credit card anywhere, especially for online transactions.

About this short piece of non-fiction written in computers and technology genre:

I started writing this non-fiction for my friend, whose pseudonym is Mr. Stark; But I ended up writing about a lot of things like evils corps. That's why I decided to publish this in archive.org, a DRM free content provider in the internet. And by the way, my pseudonym is 'kid'.